Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of controlling security of data in a storage system having a local disk system and a remote disk system comprising:

in the local disk system:

when a write of data is to be made to the local disk system retrieving a previously stored encryption key;

encrypting the data;

transferring the data to the remote disk system; then

in the remote disk system:

determining whether the data is to be stored in an encrypted form;

determining an address for storage of the data in the remote disk system;

if the data is to be stored in a decrypted form, decrypting ~~the data;~~ and writing the data in the remote disk system; ~~and~~

if the data is to be stored in an encrypted form, writing the data in the remote disk system without decrypting the data; and

notifying the local disk system that the step of writing the data is complete,

wherein the local disk system is coupled to a host computer to allow the host computer to access data stored in the local disk system.

2. (Currently Amended) A method as in claim 1 further comprising a step of maintaining an encryption control table on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system,

wherein the data transfer between the local disk system and the remote disk system occurring via a communication link that couples the local disk system to the remote disk system, so that the local disk system may send the data to the remote disk system without direct involvement from the host computer

wherein a first key is assigned to a first set of volumes in the local disk system, and a second key is assigned to a second set of volumes in the local disk system, each of the first and second set of volumes including one or more volumes.

3. (Original) A method as in claim 2 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local disk system.

4. (Original) A method as in claim 2 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote disk system.

5. (Original) A method as in claim 3 wherein the encryption key is applicable to less than all of the storage on the local disk system.

6. (Original) A method as in claim 4 wherein the encryption key is applicable to less than all of the storage on the remote disk system.

7. (Original) A method as in claim 3 wherein the encryption key is applicable to at least one disk on the local disk system.

8. (Original) A method as in claim 7 wherein the encryption key is applicable to at least one disk on the remote disk system.

9. (Currently Amended) A method for changing an encryption key while operating a storage system having a local disk system and a remote disk system comprising:

storing an encryption key in a memory in the local disk system;

transmitting the encryption key to the remote disk system and storing it in a memory there;

in the local disk system determining a boundary for use of the encryption key;

in the remote disk system receiving the boundary from the local disk system;

in both the local and the remote disk system, determining a relationship of present operations to the boundary;

in both the local and the remote disk system waiting for the boundary, and then changing the encryption key for data stored thereafter.

10. (Original) A method as in claim 9 wherein operations before the boundary are performed using a first encryption key and operations after the boundary are performed using a second encryption key.

11. (Original) A method as in claim 9 wherein the boundary is defined by counting input/output operations and using the count to define the boundary.

12. (Currently Amended) A method for changing an encryption key while operating a storage system having a local disk system and a remote disk system, the method comprising:

storing an encryption key in a memory in the local disk system;

transmitting the encryption key to the remote disk system and storing it in a memory there;

issuing split request ~~splitting~~ from the local disk system ~~from~~ to the remote disk system to allow them to operate independently;

using a new encryption key to begin storing data in the local disk system after issuing the split request; ~~and~~

using a new encryption key to begin storing data in the remote disk system after receiving the split request; and

resynchronize the local disk system and the remote disk system.

13. (Currently Amended) A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

maintaining a control table in each of the local disk system and the remote disk system;

determining a boundary in the local disk system where encryption is to be switched to an opposite state;

in the remote disk system receiving ~~determining~~ a corresponding boundary from ~~in~~ the remote disk system;

in both the local and the remote disk system, determining a relationship of present operations to the boundary;

in both the local and the remote disk system waiting for the boundary, and then changing the switching the encryption to the opposite state.

14. (Original) A method as in claim 13 wherein operations before the boundary are either encrypted or not encrypted, and operations performed after the boundary are either not encrypted or encrypted oppositely to those operations performed before the boundary.

15. (Original) A method as in claim 14 wherein the boundary is defined by counting input/output operations and using the count to define the boundary.

16. (Currently Amended) A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

storing an encryption key in a memory in the local disk system;

transmitting the encryption key to the remote disk system and storing it in a memory there;

splitting the local disk system from the remote disk system to allow them to operate independently;

switching encryption to an opposite state from a previous state after splitting the local disk system and remote disk system; and

re-synchronizing the local disk system and the remote disk system.

17. (Currently Amended) A storage system comprising:

a local disk system including a plurality of volumes of media for storing data~~;~~ , said local disk system being coupled to a host computer to enable the host computer to access said volumes;

a remote disk system including a plurality of volumes of media for storing data; and

~~a first computer program operating on the local system to determine whether encryption is to be employed in storage of data on the local system, and if so, retrieving an encryption key from storage and using the key to encrypt the data to be stored;~~

a communications link coupling the local system to the remote system~~; and~~ ,

wherein the local disk system determines whether encryption is to be employed in the data on the local disk system, and if so, encrypts the date to be transferred to the remote disk system, and

wherein the remote disk system determines whether to store the data in either encrypted form or unencrypted form and stores the data in that form in the remote disk system, and notifies the local disk system that the data has been stored.

~~a second computer program operating on the remote system to store the data in either encrypted form or unencrypted form based and storing the data in that form in the remote system, and notifying the local disk system that the data has been stored.~~

18. (Original) A system as in claim 17 further comprising an encryption control table stored on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local system and the remote system.

19. (Original) A system as in claim 18 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local system.

20. (Original) A system as in claim 19 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote system.

21. (Original) A system as in claim 20 wherein the encryption key is applicable to less than all of the storage on the local system.

22. (Original) A system as in claim 21 wherein the encryption key is applicable to less than all of the storage on the remote system.

23. (Currently Amended) A storage system ~~having a local system and a remote system, and~~ having changeable encryption keys, comprising:

a local disk system;

a remote disk system; and

~~a local memory which stores an encryption key in the local system;~~

a communications link connecting the local disk system to the remote disk system for transmitting the encryption key from the local disk system to the remote disk system~~;~~ ,

~~a remote memory which stores the encryption key in the remote system;~~

wherein ~~a first computer program in~~ the local disk system ~~which~~ determines a boundary for use of the encryption key; and

wherein the remote disk system receives the boundary from the local disk system; and

wherein ~~in~~ both the local and the remote disk system, ~~a second computer program for determining~~ determine a relationship of present operations to the boundary, and ~~changing~~ change the encryption key for operations occurring after the boundary.

24. (Canceled)

25. (Canceled)

26. (Currently Amended) A system for controlling encryption in a storage system having a local system and a remote system comprising:

a local memory storing an encryption key in the local system;

a communications link for transmitting the encryption key to the remote disk system and storing it in a remote memory there;

a first computer program for splitting the local system from the remote system to allow them to operate independently;

a switch for changing encryption to an opposite state from a previous state after splitting in the local disk system and remote disk system; and

a second computer program for re-synchronizing the local system and the remote system.

27. (Currently Amended) A method of controlling security of data in a storage system having a local disk system and a remote disk system comprising:

in the local disk system:

receiving a data update request from a host computer connected to the local disk system wherein said data update request includes a location of a fist portion of the local disk system;

assigning a key to ~~a~~ the first portion of the local disk system;

encrypting the data stored in the first portion of the local disk system;

transferring the encrypted data to the remote disk system; then

in the remote disk system:

decrypting the data using the assigned key; and

writing the decrypted data into a second portion of the remote disk system.

28. (Original) A method as in claim 27 wherein the first portion comprises at least a volume of the local storage system and the second portion comprises at least a volume of the remote disk system.

29. (Original) A method as in claim 28 wherein the first portion comprises a group of volumes of the local storage system, and the second portion comprises a group of volumes of the remote storage system.

30. (Currently Amended) A storage system comprising:

a local disk system including a plurality of volumes of media for storing data~~;~~, wherein the local disk system is connected to a host computer;

a remote disk system including a plurality of volumes of media also for storing data;

a communications link coupling the local disk system to the remote disk system,

wherein ~~a first computer program operating on~~ the local disk system ~~to~~ retrieves selected data from ~~storage~~ one of the volumes on the local system, ~~and~~ encrypts that selected data using an encryption key~~;~~ , and transmits the encrypted selected data to the remote disk system,

~~a communications link coupling the local system to the remote system for transmitting the encrypted selected data to the remote system;~~ and

wherein ~~a second computer program operating on~~ the remote disk system ~~to~~ decrypts the selected data received from the communications link and stores that selected data in unencrypted form in one of the volumes of media the remote system.

31. (Original) A system as in claim 30 further comprising an encryption control table stored on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local system and the remote system.